TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE

PRESIDÊNCIA

PORTARIA Nº 195/2026/PRES

Institui o fluxo do processo de trabalho "Gerenciar Privacidade Desde a Concepção (Privacy by Design)" no âmbito do Tribunal Regional Eleitoral do Rio Grande do Norte e dá outras providências.

A PRESIDÊNCIA DO TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE, no uso de suas atribuições legais e regimentais,

Considerando o disposto na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), especialmente os princípios da prevenção, da segurança e da responsabilização e prestação de contas previstos no art. 6º;

Considerando as diretrizes do Conselho Nacional de Justiça relativas à governança, à segurança da informação e à proteção de dados pessoais no âmbito do Poder Judiciário;

Considerando o Acórdão TCU nº 1.372/2025 – Plenário, que orienta os órgãos da Administração Pública à adoção de mecanismos estruturados de gestão de riscos e à incorporação da proteção de dados pessoais ao ciclo de governança institucional;

Considerando o Plano Estratégico da Justiça Eleitoral do Rio Grande do Norte – PEJERN 2021-2026, especialmente a iniciativa de implementação de mecanismos voltados à proteção de dados pessoais (AC3.5);

Considerando a necessidade de implementar a diretriz da Política de Proteção de Dados Pessoais do Tribunal Regional Eleitoral do Rio Grande do Norte relativa à adoção dos conceitos de privacidade desde a concepção (*Privacy by Design*) e privacidade por padrão (*Privacy by Default*) nos processos, projetos, contratações e sistemas da instituição,

RESOLVE:

CAPÍTULO I

DAS DISPOSIÇÕES GERAIS

Art. 1º Fica instituído o processo de trabalho "Gerenciar Privacidade Desde a Concepção (*Privacy by Design*)" do Tribunal Regional Eleitoral do Rio Grande do Norte (TRE-RN), nos termos

dos Anexos I, II, III e IV, que tratam do fluxo procedimental e dos instrumentos de avaliação de riscos.

Art. 2º O processo de que trata esta Portaria tem por objetivo assegurar que qualquer projeto, sistema, serviço ou contratação do TRE-RN que envolva tratamento de dados pessoais seja submetido a uma avaliação prévia e progressiva de privacidade, incorporando medidas de proteção desde a fase de concepção, em observância ao disposto na Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018), em seu art. 46, § 2º.

Art. 3º Para os fins desta Portaria, consideram-se:

I – *Privacy by Design*: a incorporação sistemática de medidas técnicas e administrativas destinadas a assegurar a proteção de dados pessoais desde a fase inicial de concepção até o encerramento do ciclo de vida do tratamento, em consonância com a LGPD e com as diretrizes institucionais de governança e gestão de riscos;

II – Formulário de Avaliação Prévia de Privacidade (FAPP): instrumento de triagem (*privacy screening*) de responsabilidade exclusiva da unidade demandante;

III – *Checklist* de Privacidade: instrumento de verificação de conformidade analisado concomitantemente pela Assessoria de Integração (ASSINT) e pela unidade técnica de segurança da informação;

IV – Relatório de Impacto à Proteção de Dados Pessoais (RIPD): instrumento de avaliação aprofundada, elaborado pela unidade demandante nos casos de alto risco;

V – Dados pessoais sensíveis: dados sobre origem racial ou étnica, convicção religiosa, opinião política, filiação sindical, saúde, vida sexual, genética ou biometria vinculados a pessoa natural (art. 5º, II, LGPD);

VI – Alto risco: nível de risco que exige o percurso completo do fluxo, incluindo a elaboração do RIPD;

VII – Risco residual alto: risco remanescente após a aplicação das medidas mitigatórias propostas.

CAPÍTULO II

DO ÂMBITO DE APLICAÇÃO

Art. 4º O disposto nesta Portaria aplica-se obrigatoriamente:

I – à concepção de novos projetos institucionais;

II – à contratação ou ao desenvolvimento de sistemas informatizados que envolvam tratamento de dados pessoais;

III – à evolução relevante de sistemas existentes;

IV – aos projetos estratégicos e sistemas críticos submetidos a revisão, ampliação ou atualização tecnológica;

V – às contratações de bens e serviços em que o fornecedor tenha acesso, ainda que indireto, a dados pessoais tratados pelo Tribunal.

§ 1º As unidades responsáveis por projetos, sistemas e contratações deverão integrar os procedimentos previstos nesta Portaria à governança institucional, à gestão de riscos e ao

planejamento estratégico do Tribunal.

§ 2º Este processo de trabalho não se aplica a iniciativas internas que não envolvam qualquer forma de tratamento de dados pessoais.

CAPÍTULO III

DAS RESPONSABILIDADES E DO FLUXO PROCESSUAL

Art. 5º As responsabilidades das unidades envolvidas no fluxo de avaliação de privacidade estão definidas no Anexo I, observando-se, em síntese:

I – à unidade demandante: o preenchimento dos instrumentos Formulário de Avaliação Prévia de Privacidade (FAPP) - Anexo II, *Checklist* de Privacidade - Anexo III e Relatório de Impacto à Proteção de Dados Pessoais (RIPD) - Anexo IV, conforme o caso;

II – à unidade responsável pela governança de proteção de dados pessoais (ASSINT): a análise concomitante do *Checklist* em relação à legitimidade, necessidade, proporcionalidade e compatibilidade do tratamento de dados pessoais com a LGPD, a coordenação metodológica da elaboração do RIPD e a cooperação na elaboração do RIPD, quando solicitada;

III – à unidade técnica de segurança da informação: a análise concomitante do *Checklist* sobre as salvaguardas propostas contra acessos indevidos, vazamentos e incidentes de segurança da informação;

IV – à alta administração, por meio dos comitês de governança competentes: a apreciação dos casos de alto risco residual e a deliberação sobre continuidade, revisão ou suspensão de projetos.

Art. 6º O FAPP é ato exclusivo da unidade demandante e deve ser preenchido antes da abertura do processo administrativo, publicação de edital, assinatura de contrato ou autorização de projeto.

§ 1º Identificada, no FAPP, a realização de tratamento de dados pessoais, a unidade demandante deverá preencher o *Checklist* para Gestores(as) de Projetos, para subsidiar a avaliação de riscos à privacidade, a definição de medidas mitigadoras e a verificação da necessidade de elaboração do RIPD.

§ 2º O FAPP que concluir pela inexistência de tratamento de dados pessoais permanecerá arquivado na unidade demandante, sem prejuízo de sua apresentação quando solicitada pelas instâncias de governança, controle ou auditoria.

Art. 7º A elaboração do RIPD, quando necessária nos termos desta Portaria, é de responsabilidade da unidade demandante, à qual compete descrever os processos de tratamento, identificar os riscos e propor as medidas de mitigação cabíveis, observada a metodologia institucional de gestão de riscos.

§ 1º A ASSINT, na condição de unidade técnica especializada em proteção de dados pessoais, apoiará metodologicamente a elaboração do RIPD, prestando orientação técnica quando necessário, e emitindo parecer conclusivo sobre o nível de risco identificado e a adequação das medidas propostas.

§ 2º A cooperação da ASSINT na elaboração do RIPD não transfere a essa unidade a prerrogativa de deliberar sobre a continuidade, revisão ou suspensão do projeto, que permanece com as instâncias de governança competentes nos casos de risco residual alto.

Art. 8º Identificada a existência de risco residual alto após a elaboração do RIPD, a matéria será submetida à análise e deliberação dos comitês de governança competentes, que poderão autorizar a continuidade da iniciativa, com ou sem a adoção de medidas adicionais de mitigação, determinar sua revisão ou suspensão, ou, constatado risco inaceitável aos direitos e liberdades dos(as) titulares, deliberar pelo arquivamento da demanda.

Parágrafo único. A ASSINT poderá solicitar o apoio do Grupo de Trabalho Técnico de apoio ao(à) Encarregado(a) pelo Tratamento de Dados Pessoais (GTT) para subsidiar a análise do RIPD e a avaliação do risco residual, especialmente quanto à adequação das medidas mitigadoras propostas.

Art. 9º Os procedimentos previstos nesta Portaria observarão os seguintes prazos:

I – o FAPP deverá ser preenchido pela unidade demandante antes do início formal do projeto, contratação, desenvolvimento, evolução ou revisão de sistema;

II – a análise do *Checklist* para Gestores(as) de Projetos será realizada concomitantemente pela ASSINT e pela unidade técnica de segurança da informação, no prazo de até 5 (cinco) dias úteis, quando o tratamento for classificado como de alto risco;

III – a análise do RIPD pela ASSINT será realizada no prazo de até 3 (três) dias úteis, contados do recebimento do relatório elaborado pela unidade demandante.

Parágrafo único. Quando o tratamento for classificado como de baixo ou médio risco, a análise do *Checklist* para Gestores(as) de Projetos será realizada concomitantemente pela ASSINT e pela unidade técnica de segurança da informação, no prazo de até 3 (três) dias úteis.

Art. 10. O FAPP que indicar tratamento de dados pessoais, bem como o *Checklist* para Gestores(as) de Projetos, o RIPD e os documentos de orientação emitidos no curso da avaliação, serão encaminhados à ASSINT, para registro e manutenção em repositório institucional de governança de dados.

CAPÍTULO IV

DA CLASSIFICAÇÃO DOS NÍVEIS DE RISCO

Art. 11. Para fins de aplicação do processo Gerenciar Privacidade Desde a Concepção (*Privacy by Design*), o tratamento de dados pessoais será classificado em níveis de risco baixo, médio ou alto, considerando-se, entre outros, a natureza dos dados tratados, o volume de titulares envolvidos, a abrangência do tratamento, o compartilhamento de dados, as tecnologias empregadas e os potenciais impactos aos direitos e liberdades dos(as) titulares.

Art. 12. Considera-se de baixo risco o tratamento de dados pessoais que, em regra:

I – envolva predominantemente dados pessoais comuns, a exemplo de nome, CPF, matrícula funcional, e-mail institucional, telefone, endereço, cargo, lotação, frequência ao trabalho, dados financeiros não sensíveis (como remuneração para fins administrativos) e histórico funcional;

II – alcance grupo limitado e determinado de titulares, com potencial reduzido de impacto em caso de incidente de segurança ou uso indevido dos dados pessoais;

III – não envolva compartilhamento externo contínuo, sistemático ou em larga escala de dados pessoais; e

IV – não compreenda decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que produzam efeitos jurídicos ou afetem significativamente os interesses dos(as) titulares.

Parágrafo único. Incluem-se nessa categoria, exemplificativamente, o cadastro interno de servidores(as), magistrados(as), estagiários(as) e colaboradores(as), os sistemas de controle administrativo de frequência e os sistemas internos de gestão que não utilizem dados do cadastro eleitoral nem permitam acesso a dados de eleitores(as).

Art. 13. Considera-se de médio risco o tratamento de dados pessoais que, em regra:

I – envolva volume significativo de dados pessoais comuns ou alcance ampla quantidade de titulares, especialmente em sistemas corporativos de gestão administrativa, financeira ou de pessoal;

II – compreenda integração ou interoperabilidade entre sistemas internos que impliquem compartilhamento ou consolidação de dados pessoais entre unidades do Tribunal;

III – preveja acesso limitado e controlado de fornecedores, prestadores de serviço ou operadores aos dados pessoais, mediante perfis de acesso restritos e observância de medidas de segurança da informação; ou

IV – contemple criação, ampliação ou alteração relevante de funcionalidades de sistemas administrativos que impliquem novas formas de coleta, utilização, compartilhamento ou armazenamento de dados pessoais.

Parágrafo único. Incluem-se entre os exemplos de tratamento de médio risco, sem prejuízo de outros casos com características semelhantes, os sistemas corporativos de gestão administrativa, orçamentária, financeira ou de pessoal que integrem dados funcionais, as ferramentas internas de análise estatística sem utilização de dados pessoais sensíveis e o compartilhamento controlado de dados pessoais entre unidades da Justiça Eleitoral.

Art. 14. Considera-se de alto risco o tratamento de dados pessoais que envolva um ou mais dos seguintes elementos:

I – dados pessoais sensíveis, inclusive dados biométricos do cadastro eleitoral;

II – tratamento em larga escala de dados de eleitores(as), candidatos(as), partidos políticos ou demais titulares;

III – interoperabilidade ou compartilhamento relevante com bases de dados externas;

IV – decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que produzam efeitos jurídicos ou afetem significativamente os interesses dos(as) titulares;

V – sistemas críticos para a atividade jurisdicional ou administrativa da Justiça Eleitoral;

VI – acesso direto de fornecedores ou operadores a bases de dados eleitorais;

VII – elevado potencial de impacto aos direitos e liberdades fundamentais dos(as) titulares dos dados pessoais; ou

VIII – tratamento de dados pessoais de crianças e adolescentes, nos termos do art. 14 da LGPD e das diretrizes da Agência Nacional de Proteção de Dados (ANPD).

Parágrafo único. Incluem-se entre os exemplos de tratamento de alto risco, sem prejuízo de outros casos com características semelhantes, os sistemas de identificação biométrica, os projetos de modernização, migração ou evolução relevante do cadastro eleitoral, o cruzamento massivo de dados com outros órgãos ou entidades, os sistemas automatizados aptos a impactar a

regularidade da inscrição eleitoral ou a situação eleitoral do cidadão, bem como projetos estratégicos ou sistemas críticos que realizem tratamento em larga escala de dados pessoais, inclusive aqueles que envolvam dados de crianças e adolescentes.

Art. 15. A classificação do nível de risco deverá observar os critérios estabelecidos no FAPP, sem prejuízo da consideração de outros elementos técnicos, jurídicos ou operacionais identificados pela ASSINT, pela unidade técnica de segurança da informação ou pelo(a) Encarregado(a) pelo Tratamento de Dados Pessoais.

Art. 16. Os exemplos de tratamentos associados a cada nível de risco possuem caráter meramente ilustrativo e não vinculante, cabendo a avaliação do caso concreto à luz da LGPD e das normas institucionais aplicáveis.

CAPÍTULO V

DAS DISPOSIÇÕES FINAIS

Art. 17. Os instrumentos produzidos no âmbito do processo Gerenciar Privacidade desde a Concepção (*Privacy by Design*), incluindo o FAPP, o *Checklist* para Gestores(as) de Projetos, o RIPD e os documentos de orientação emitidos pelas unidades técnicas competentes, deverão ser registrados e mantidos de modo a assegurar sua integridade, rastreabilidade, auditabilidade e disponibilidade para fins de governança, gestão de riscos e auditoria interna e externa.

Art. 18. Os instrumentos convocatórios, contratos, acordos, termos de referência e demais instrumentos congêneres firmados pelo Tribunal que envolvam tratamento de dados pessoais ou possibilitem o acesso a dados pessoais por fornecedores, operadores ou terceiros deverão conter cláusula específica de proteção de dados pessoais, em conformidade com a LGPD e as orientações emitidas pela ASSINT.

§ 1º A ausência de tratamento ou de acesso a dados pessoais no âmbito da contratação deverá ser justificada pela unidade demandante nos autos do processo administrativo correspondente.

§ 2º A inclusão de cláusula de proteção de dados pessoais não afasta a necessidade de adoção das demais medidas de governança, segurança da informação e privacidade previstas nesta Portaria.

Art. 19. A revisão do RIPD deverá ocorrer, no mínimo, a cada 2 (dois) anos ou sempre que houver alteração relevante no tratamento de dados pessoais, especialmente quanto à finalidade, às categorias de dados tratados, aos titulares, às tecnologias empregadas ou ao compartilhamento de dados.

Art. 20. As iniciativas em andamento na data de publicação desta Portaria deverão ser submetidas ao fluxo de avaliação de privacidade no prazo de 120 (cento e vinte dias), priorizando-se os projetos de alto risco.

Art. 21. Os casos omissos serão resolvidos pela Presidência.

Art. 22. Esta Portaria entra em vigor na data de sua publicação.

Assinado e datado eletronicamente

Desembargadora **Maria Lourdes Azevêdo**
Presidente

Documento assinado eletronicamente por **Maria de Lourdes Medeiros de Azevêdo**, **Presidente do TRE-RN**, em 04/08/2026, às 15:59, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-rn.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=2546035&crc=A2243E3E informando, caso não preenchido, o código verificador **2546035** e o código CRC **A2243E3E**.

Anexo I - Desenho do fluxo processual

Anexo II - Modelo do Formulário de Avaliação Prévia de Privacidade (FAPP)

Anexo III - Modelo do Checklist de Privacidade para Gestores de Projetos

Anexo IV - Modelo do Relatório de Impacto à Proteção de Dados Pessoais (RIPD)